

**PATENT APPLICATION IN THE U.S. PATENT AND TRADEMARK OFFICE**

**FOR**

**METHOD AND SYSTEM FOR THIRD PARTY RESOURCE  
PROVISIONING MANAGEMENT**

**BY**

**JEFFREY C. CURIE  
KAI MILDENBERGER  
FRANK YEH, JR.**

**Background**

**1. Field of the Invention**

The present invention relates, generally, to resource provisioning management (RPM) systems, and, in preferred embodiments, to third party providers of resource provisioning management services.

**2. Description of Related Art**

A common use of communication networks is to provide users access to network resources such as software, electronic data, or files in storage systems or databases connected to the network. As the number of users on a given network increases, there is often a need to control user access rights to resources on the network. However, as the number and type of resources available over the network increase, the difficulty in managing access rights to such resources tends to increase. Further difficulties arise where resources are in remote locations, accessible to users over a distributed network, such as the Internet.

Network environments often involve a variety of network users, where the users may be grouped or categorized by a relation or role that the user serves in the environment. For example, in an engineering or technical development company environment, users of the company's computer network may include company officers, directors, managers, engineers,

technical support staff, office support staff, accounting department staff, information technology (IT) department staff, contractors, consultants, temporary employees or other relation-based or role-based groups or categories of network users. Other companies, organizations or network environments may have other relation or role-based groups of users.

5 Each user may have a need to access certain network resources in connection with the user's relation or role. In addition, it may be desirable to restrict users with certain relations or roles from access to certain resources, for example, for security, privacy or other reasons.

Depending on the network environment, other types of resources may also be allocated to (or restricted from) users, based on the user's relation or role in the environment.

10 For example, in the engineering or development company environment described above, users may be allocated such resources as telephones, telephone accounts, computers, Internet accounts, e-mail accounts, office equipment and supplies, laboratory or engineering equipment and supplies, or other resources, based on the user's role or relation with the company.

15 In many conventional businesses or organizations, specific personnel perform the function of provisioning users according to their roles. For example, an office administrator may place an order with the organization's information technology (IT) department to have a computer, telephone, voice mail, e-mail, and certain applications and databases available on the day a new user joins the organization. Individuals from the IT department would then manually set up these resources. Other office personnel may bring  
20 desks, chairs, and cabinets from storage and set up the user's office. Over the course of time, the user's relationship or roles within the organization may change, for example, as the user is transferred, promoted, demoted or terminated from the organization. As a user's relationship or role with the organization changes, the user's needs or rights to access resources may change.

25 The burden on the office administrator and office personnel to manually administer user access to resources in the above example is typically dependent on the size of the organization (the number of users) and the rate at which users join or leave the organization or otherwise change roles. To improve efficiency and reduce the burden on the office administrator and office personnel, some organizations have used software applications

which automate or partially automate some of the tasks relating to provisioning certain, limited types of resources to users.

Role Based Access Control (RBAC) is one form of automatic provisioning that has become commercially available. RBAC provides permissions (access rights) to a user to  
5 access certain accounts (files, web pages, etc.) available over the network, based on a person's role in the organization. For example, a file or folder may be viewed only by its creator, or may be accessible to a larger group of users through an organization's network, depending on the permission rights established for that file or folder. In conventional RBAC systems, these permissions are based on a person's role within the organization.

10 However, modern organizations may be structured along several intersecting lines. For example, organizations may be structured according to title (presidents, vice-presidents, directors, managers, supervisors, etc.), technology (electronics, mechanical, software, etc.), project (product A, B, C, etc.), location (Irvine, New York, etc.) and the like. A single user may appear in several or all of these organizational structures, and thus may be  
15 in a somewhat unique overall role as compared to other users in the organization. Because this may require that many users be provisioned uniquely, many unique roles would have to be defined in the system to automate such provisioning. Furthermore, conventional RBAC only provisions "soft" resources such as accounts, applications, databases, files, Web pages, and the like, as opposed to "hard" resources such as telephones, computers, desks, and the like.

20 The software applications which automate or partially automate some of the tasks relating to provisioning certain, limited types of resources to users are operable on a communication network for provisioning users with resources according to established criteria. Systems employing such software applications will be generally referred to herein as RPM systems.

25 Although the third party service providers or managed services (collectively known as managed resources) may have user management consoles which enable a human to make changes to the managed resource, the consoles or interfaces may be incompatible with the RPM system. Because of this, software agents may be deployed as translators between the RPM system and the managed resources. The agent, in essence, replaces human intervention  
30 with automated steps that perform essentially the same function. The agent is capable of

receiving a message or request from the RPM system, and translating the request to code that can interface with the Application Programming Interfaces (APIs) of the managed resource. After the managed resource performs the particular function of the request, the managed resource may pass values to the agent, which may then communicate the values back to the  
5 RPM system.

Unfortunately, the implementation of an RPM system may require resources that are cost-prohibitive for some companies or organizations. Implementation of an RPM system typically requires system servers, terminals, system software, agents and other items associated with a communications network. Expenditures for such items can be tremendous,  
10 costing anywhere from tens of thousands to hundreds of thousands of dollars. These costs may be overwhelming for companies or organizations of modest means, thereby putting acquisition and implementation of an RPM system out of reach.

Also, the implementation of an RPM system typically requires a commitment to personnel for the operation of the system. The cost required to hire and train such personnel  
15 and the costs for associated overhead may discourage some companies or organizations from implementing an RPM system altogether. Thus, without a viable alternative for RPM services, these companies and organizations cannot benefit from an RPM system.

Companies and other organizations who lack the resources for or who are otherwise discouraged from acquiring and implementing an RPM system could benefit greatly  
20 from third parties who function as providers of RPM services. Up until now, however, a system and method for providing third party RPM services has not existed. Generally, an RPM system and method has heretofore been implemented within an organization utilizing resources in an enterprise or application service provider environment.

Tremendous benefit could also be obtained by companies and other  
25 organizations utilizing third party RPM service providers if the resources being provisioned could be shared among such companies or organizations. Such sharing among affiliated companies could provide cost savings and administrative efficiency. Again, however, up until now, a mechanism for sharing resources among affiliate companies or organizations utilizing third party RPM service providers has not existed.

A need also exists for a public infrastructure generally in the RPM sector. There does not currently exist any third party RPM service provider delivering provisioning services such as identity, entitlement, policies and roles for the general public to utilize when the need for resource provisioning arises.

5 **Summary**

Therefore, embodiments of the present invention relate to systems and methods for provisioning resources of a plurality of organizations using a single logical server, where each organization may have internal resources.

Such a method may comprise the steps of establishing a set of attributes,  
10 organizational information, and user roles for each organization; defining a plurality of resource provisioning policies for each organization based on selected attributes, organizational information, and user roles; receiving attribute information, organizational information, and user role information from each organization for a particular user, resource, or database; determining which resource provisioning policies are applicable to the user based  
15 on the received user role information, organizational information, and attribute information; and provisioning the user from a remote, centralized location with resources based on the applicable resource provisioning policies.

The method may also include provisioning over a network and provisioning users with external resources.

20 A method for provisioning resources of a plurality of organizations using a single logical server, each organization having internal resources may also comprise the steps of establishing a set of attributes, organizational information, and user roles for each organization; defining a plurality of resource provisioning policies for each organization based on selected attributes, organizational information, and user roles; receiving attribute  
25 information, organizational information, and user role information from each organization for a particular user, resource, or database; determining which resource provisioning policies are applicable to users based on the received user role information, organizational information, and attribute information; grouping each organization together into a resource exchange; and

cross-provisioning users from a remote, centralized location with resources from organizations within the resource exchange based on the applicable resource provisioning policies.

The method may also include the step of providing a translational map for organizations within the resource exchange. Further, the method may include the step of providing high level authentication of organizations within the resource exchange. The method may further include the step of providing identity synchronization of organizations within the resource exchange. The method may further include the step of providing an audit trail for organizations within the resource exchange, and may further include the step of providing anonymity for organizations within the resource exchange.

A method for provisioning resources of a plurality of organizations using a server in a public provision infrastructure may also comprise the steps of establishing a set of attributes, organizational information, and user roles for each organization having resources; defining a plurality of resource provisioning policies for each organization having resources based on selected attributes, organizational information, and user roles; receiving attribute information, organizational information, and user role information from each organization for a particular user, resource, or database; receiving attribute information, organizational information, and user role information from members of a general public desiring use of a resource within the public provisioning infrastructure; generating a resource provisioning ticket for the members of the general public; determining which resource provisioning policies are applicable to users based on the received user role information, organizational information, and attribute information; and forwarding the provisioning ticket to a vendor of a particular resource.

A system for provisioning resources of a plurality of organizations may comprise a third party resource provisioning management service provider; a server for provisioning resources, wherein the server is operated by a third party resource provisioning management service provider; internal resources belonging to each organization; and a network providing a link between the server and the internal resources; wherein the third party resource provisioning management service provider provisions the internal resources of each organization over the network at the request of the organization.

The system may further comprise external resources, wherein the external resources are provisioned for each organization.

A system for provisioning resources of a plurality of organizations may also comprise a third party resource provisioning management service provider; a server for  
5 provisioning resources, wherein the server is operated by a third party resource provisioning management service provider; a resource exchange made up of the plurality of organizations, each organization having internal resources; and a network providing a link between the server and the internal resources, wherein the third party resource provisioning management service provider cross-provisions the internal resources of each organization within the resource  
10 exchange over the network at the request of each organization.

The system may further comprise a translational map for organizations within the resource exchange, means for each high level authentication of organizations within the resource exchange, means for identity synchronization of organizations within the resource exchange, and means for providing an audit trail for organizations within the resource  
15 exchange.

A system for provisioning resources of a plurality of organizations may also comprise means for establishing a set of attributes, organizational information, and user roles for each organization having resources; means for defining a plurality of resource provisioning policies for each organization having resources based on selected attributes, organizational  
20 information, and user roles; means for receiving attribute information, organizational information, and user role information from each organization for a particular user, resource, or database; means for receiving attribute information, organizational information, and user role information from members of a general public desiring use of a resource within the public provisioning infrastructure; means for generating a resource provisioning ticket for the  
25 members of the general public; means for determining which resource provisioning policies are applicable to users based on the received user role information, organizational information, and attribute information; and means for forwarding the provisioning ticket to a vendor of a particular resource.

These and other objects, features, and advantages of embodiments of the invention will be apparent to those skilled in the art from the following detailed description of embodiments of the invention, when read with the drawings and appended claims.

### **Brief Description of the Drawings**

5           FIG. 1 is a diagram of an external view of an Application Service Provider (ASP) environment embodiment of the present invention.

FIG. 2 is a diagram of an external view of a Corporate Enterprise environment embodiment of the present invention.

10           FIG. 3 is a diagram of logical architecture of a system according to an embodiment of the present invention.

FIG. 4 is a diagram of a component arrangement of a system according to an embodiment of the present invention.

FIG. 5 is a diagram of an example deployment of a system according to an embodiment of the present invention.

15           FIG. 6 is a diagram of another example deployment of a system according to an embodiment of the present invention.

FIGS. 7A-E are sequence diagrams of interactions relating to authenticating a user, adding a user, provisioning a service for a user, provisioning services for a new user based on policy, and synchronizing services and enforcing policy violations.

20           FIG. 8 is diagram of graphical interfaces in a sequence relating to a provisioning process.

FIG. 9 is a diagram of a generalized architecture of a resource provisioning management system according to an embodiment of the present invention

25           FIG. 10 is a diagram of a resource provisioning management system utilizing a centralized server according to an embodiment of the present invention.

FIG. 11A is a flow diagram of resource provisioning management using a centralized server according to an embodiment of the present invention.



FIG. 11B is another flow diagram of resource provisioning management using a centralized server according to an embodiment of the present invention.

FIG. 12 is a diagram of a resource provisioning management system utilizing a centralized server and external resources according to an embodiment of the present invention.

5        FIG. 13 is a diagram of a resource provisioning management system utilizing a centralized server providing cross-provision of affiliate resources in a resource exchange according to an embodiment of the present invention.

10       FIG. 14A is a flow diagram of a resource provisioning management method utilizing a centralized server providing cross-provisioning of affiliate resources in a resource exchange according to an embodiment of the present invention.

FIG. 14B is another flow diagram of a resource provisioning management method utilizing a centralized server providing cross-provisioning of affiliate resources in a resource exchange according to an embodiment of the present invention.

15       FIG. 15 is a diagram of a resource provisioning management system utilizing a centralized server providing a public provisioning infrastructure according to an embodiment of the present invention.

FIG. 16 is a flow diagram of a resource provisioning management method utilizing a centralized server providing a public provisioning infrastructure according to an embodiment of the present invention.

20       FIG. 17 is a diagram of various levels of a resource provisioning management system utilizing a centralized server according to an embodiment of the present invention.

### **Detailed Description of Preferred Embodiments**

25       In the following description of preferred embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the preferred embodiments of the present invention.

### System Overview

As described above, embodiments of the present invention relate to a system operable on a communication network for provisioning users with resources based on policies, roles and attributes. Embodiments of the present invention will be generally referred to herein  
5 as a resource provisioning management (RPM) system, or simply "the system."

The system may be implemented with software applications and modules deployed on various processor or computer systems connected for communication over one or more network or non-network links. As described in more detail below, the processors in which the modules and applications are deployed may differ from system embodiment to  
10 system embodiment. In addition, the types of users, administrators and other entities that interact with the system may differ from system embodiment to system embodiment. Preferred embodiments of the system are designed to provide a high level of flexibility to accommodate the needs of a variety of potential applications of use.

Two representative examples of system environments in which embodiments of  
15 the present invention operate are shown in FIGS. 1 and 2, respectively. FIG. 1 shows a generalized representation of an Application Service Provider (ASP) environment embodiment, while FIG. 2 shows a generalized representation of an Enterprise environment embodiment of the system. In each of FIGS. 1 and 2, a platform computer system 10 is coupled for communication with a plurality of user computers, administrator computers and  
20 other entities over a network 12, depending upon the needs of the system. Further entities, including external systems, databases and directories, third party service providers, managed services and system administrators may be coupled for communication to the platform system 10 through the same network or through other networks or dedicated communication links, depending upon the needs of the system. While a number of such entities are shown and  
25 described with respect to embodiments disclosed herein, it will be understood that further system environment embodiments of the invention need not include all of the entities described herein.

The network environment may also include one or more network servers, routers and other network structure and devices (not shown). A network environment may  
30 comprise a local area network (LAN), for example, within an office or building. In other

embodiments, the network environment may comprise a wide area network (WAN) including, but not limited to, the Internet.

The platform system 10 may be implemented, for example, with one or more processors or computers which include or operate with associated memory and software modules and applications to carry out various functions described herein. The platform system 10 carries out various functions associated with provisioning users with resources based on policies, roles, organizational information, and attributes, as described below. Further functions may be carried out on processors or computers associated with the users, administrators, and service providers, for example, implemented by software running on those computers, as described below. Embodiments of the present invention can therefore run on a cluster of computers or on a single computer. These computers may or may not have multiple processors.

Users, and users acting in administrator roles, may operate computers which may include suitable processors, memory devices and user interface devices, such as, but not limited to, display devices, keyboards, mouse devices, or the like, to allow users to obtain and communicate information over the network or other communication link. Suitable software may be stored at, or be accessible to, the user and administrator Web browsers or computers, to provide user and administrator interface functions and to allow communication of electronic information and content, such as data, files, programs and other software over the network, in accordance with well known network communication technology. In addition, software for implementing functions associated with the user and administrator according to embodiments of the present invention may also be stored at, or be accessible to, the user and administrator Web browsers, respectively.

The system 10 provides a platform for defining policies and provisioning services to a user interacting with the system, or a user interacting with the network on which the system is operating. The system may designate and track the types of services as well as the types of access to these services for a large number of users. In the generalized examples of FIGS. 1 and 2, the platform system 10 may receive requests for services from user computers. The platform system 10 may also receive information from administrator computers relating to, for example, authorizations of users' requests or changes in users,

policies or roles. The platform system 10 may also provide information to the administrator Web browsers or computers, including, for example, reports on operation and service usage. The platform system 10 may provide requests, instructions, or other information to service providers or managed services computers related to providing services to the users, based on user requests, policies, roles, organizational information, and attributes. The platform system 10 may control access to services, such as data, files, programs or other electronic information from database or storage systems to the users, based on user requests, policies, roles, organizational information, and attributes.

As described above, a system according to the FIG. 1 embodiment is deployed in an ASP environment. An ASP may be described as an organization that deploys, hosts and manages access to applications such as software and other resources to multiple parties from a centrally managed facility. The applications are typically delivered over networks, including, but not limited to the Internet, on a subscription basis.

In the ASP environment, one or more users within the ASP may be designated as RPM system administrators 14 with access rights greater than other users at the same company. RPM system administrators, like other users at the same company, are capable of performing operations in accordance with policies put in place by the ASP customer, which may be based on role and organizational information for each user. However, these RPM system administrators are additionally provided with certain system configuration responsibilities, including selecting the processors on which certain modules or applications of the system are deployed, as described below. In addition, an RPM system administrator may be able to manage, for example, organizations, users, services, roles, workflow rules, policies and the system itself. An RPM provisioning system administrator may also generate reports to audit the current and historical status of the system, and may also be authorized to manage different portions of the system's data by being granted permission to access such data. The responsibilities of any given RPM system administrator may range from organization management only, to entire system management, depending upon the permission or access rights provided to the given RPM system administrator.

The system in FIG. 1 may also interface, for example, with one or more Customer End-Users 16, Customer Administrators 18, and Customer Supervisors 20. In the

illustrated example, the interfaces for the Customer End-User 16, Customer Administrator 18, and Customer Supervisor 20 are Web enabled for connection over the Internet 12.

A Customer End-User 16 is a user having access to resources in accordance with policies put in place by the customer. A Customer End-User 16 may be an employee of an ASP's customer who is provided access to certain ASP resources. A Customer End-User 16 would typically be authorized only to perform self-administration of its own personal and account information stored in a Lightweight Directory Access Protocol (LDAP) Directory server (not shown in FIG. 1) by communicating requests for provisioned services/resources over the network using a Web browser.

A Customer Administrator 18, as shown in FIG. 1, is also a user having access to resources in accordance with policies put in place by the customer. A Customer Administrator 18 may be an employee of an ASP's customer who is responsible for administering portions of a customer's organization, such as managing organizational and user information and, is therefore provided with permissions or access rights to appropriate system data to perform such functions. For example, a Customer Administrator may define and manage use of user roles and policies and, thus, may be provided with permission or access rights to the LDAP Directory Server.. Thus, a Customer Administrator may define or change users, roles, policies, organization hierarchy or the like. A Customer Administrator may also generate reports to audit the current and historical status of the system, and therefore may be provided with permission or access rights to the RPM system server containing a report engine 150 (see FIG. 3). A Customer Administrator 18 typically would be authorized to manage different portions of the system's data by being granted permission to access such data. The responsibilities of a Customer Administrator 18 may range from organization management only, to entire system management, depending upon the permission rights granted to the Customer Administrator.

A Customer Supervisor 20, as shown in FIG. 1, is also a user having access to resources in accordance with policies put in place by the customer. A Customer Supervisor 20 may be an employee of an ASP's customer who is responsible for managing or supervising groups of users in the customer organization. A Customer Supervisor 20 may delegate responsibilities to another Customer Supervisor. In preferred embodiments, the delegation of

responsibility may be authorized for a pre-defined period of time. A Customer Supervisor 20 may make changes to a roster of current users and approve requests made by users, where such requests require approval. A Customer Supervisor 20 may also generate reports to audit the current and historical status of the system. It should be understood that, in preferred  
5 embodiments, reports are not stored. Rather, they are generated as needed, and if a user wants to store a report, it would have to be saved to the user's Web browser.

FIG. 1 also indicates that the system may interface with one or more External Systems 22. An External System 22 may be any ASP system that may wish to retrieve customer or managed resource information that is managed by the system 10. This may be  
10 accomplished via a direct interface to an RPM directory (see reference character 58 in FIG. 3) used by the system 10 to store such information.

As illustrated in FIG. 1, the system may also interface with one or more Customer Datastores 24. In preferred embodiments, this interface is Internet capable. A Customer Datastore 24 may be a relational database or directory that stores ASP customer  
15 information. Note that customer-relevant data such as the customer's organization, roles, account information, and user information is stored in the directories within the Customer Datastores 24, while in-progress workflow information, audit logs, historical audit trail information (e.g., requests that have been approved), system state information (e.g. workflow state, requests that have not yet been approved), and information about remote services is  
20 stored in the databases within the Customer Datastores 24.

The system 10 may also interface, for example, with a Managed Service 26, as shown in FIG. 1. In preferred embodiments, this interface is Internet capable. A Managed Service 26 may be an application, device or datastore that the system 10 proactively manages. A Managed Service may comprise a network device that has an account maintenance system,  
25 such as an RPM system, an operating system, an application (e.g., a human resources (HR) system, enterprise resource planning (ERP) system, etc.), public key infrastructure (PKI) certificates, databases, financial services, and the like. The Managed Service's system may function independently. Thus, the datastore for the system 10 and that of a Managed Service may be synchronized periodically or at defined or irregular intervals, for example, to update  
30 the datastore.

The system may also interface, for example, with a Third Party Service Provider 28, as shown in FIG. 1. In preferred embodiments, this interface is Internet capable. A Third Party Service Provider 28 may be an external organization that provides services that may be provisioned through the system 10. A Third Party Service Provider 28 may be, for example, a credit card service that provides credit cards or credit accounts that are provisioned through the system 10. As another example, a Third Party Service Provider 28 may be a telephone service company that provides telephone line accounts that are provisioned through the system 10. It should be understood that these are merely representative examples. Many other types of services may be provided by a Third Party Service Provider in accordance with further system embodiments.

The system 10 may also interface, for example, with a Partner System 30, as shown in FIG. 1. In preferred embodiments, this interface is Internet capable. A Partner System 30 may be similar or identical to the system 10, but used by a business partner or customer and integrated into the system 10. Thus, the Partner System 30 represents a system-to-system interface which, in preferred embodiments, may be used to provide the seamless integration of multiple systems.

As described above, a system according to the embodiment of FIG. 2 is deployed in an Enterprise environment. An enterprise may be any organization that desires or requires management and administration of its resources, including, but not limited to, companies, firms, educational organizations, governmental organizations, or other groups or associations. In the FIG. 2 embodiment, the system 10 supports the same capabilities described above with respect to FIG. 1, but with some differences for different kinds of users.

For example, the system 10 may interface with a System Administrator 50 in a manner similar to the RPM system administrator interface described with respect to FIG. 1.

The System Administrator 50 may be an employee of the Enterprise, and may have responsibility for configuring the system. A System Administrator 50 may be able to manage organizations, users, services, roles, workflow rules, policies, and the system itself. A System Administrator 50 may also generate reports to audit the current and historical status of the system. A System Administrator 50 may be authorized to manage different portions of the system's data by being granted permission to access such data. The responsibilities of a

System Administrator 50 may range from organization management only, to entire system management.

Instead of Customer End-Users, Customer Administrators and Customer Supervisors described with respect to FIG. 1, the environment in FIG. 2 includes Employees (or Partners) 52, Employee Administrators 54, and Supervisors 56. Each may interface with the system 10, and are preferably web enabled for interfacing with system 10 over the Internet. An Employee may be an employee of the enterprise. An Employee 52 is a user having access to resources in accordance with policies put in place by the enterprise. Typically, an Employee may only be authorized to perform self-administration of the Employee's own personal information.

An Employee Administrator 54, as shown in FIG. 2, may be an employee of the Enterprise who is responsible for Enterprise employee administration. An Employee Administrator 54 is a user having access to resources in accordance with policies put in place by the Enterprise, who is responsible for managing the Enterprise's organizational and user information. This may involve defining, changing and managing user roles and policies. An Employee Administrator 54 may also generate reports to audit the current and historical status of the system. An Employee Administrator 54 may be authorized to manage different portions of the system's data by being granted permission to access such data. The responsibilities of an Employee Administrator 54 may range from organization management only, to entire system management.

An Enterprise Supervisor 56 may be an employee of the Enterprise who is responsible for managing groups of users within the Enterprise. Typically, an Enterprise Supervisor 56 may make changes to users and approve requests made by users. An Enterprise Supervisor 56 may also generate reports to audit the current and historical status of the system.

FIG. 2 also indicates that the system may interface with a Directory 58. A Directory 58 may be used by the system to store organizational information, user or employee information, partner information, role information, account information, resource information or the like. In one embodiment, the Directory is an LDAPv3 directory. The directory may be supplied by an Enterprise customer, or may be installed solely for the system 10.



As illustrated in FIG. 2, the system may interface with a Human Resources Datastore 60. A Human Resources Datastore 60 may be a database or directory that stores Enterprise employee and partner information.

The system 10 may also interface with a Partner System 62, Third Party Service Providers 64 and Managed Services 66, in a manner similar to that described above with respect to the Partner Systems 30, Third Party Service Providers 28 and Managed Services 26 in FIG. 1.

The system 10 in FIGS. 1 and 2 may be used to manage the provisioning of a variety of services or resources to users. A service may be any type of resource that may be accessed one or more times by users of the system. For example, a cellular telephone account or an account with a credit card company may be services. Using these services as examples, the system may, for example, designate that certain users have access to a cellular telephone account and a credit card account, and may track the usage by the user of these accounts. The system may also set various rules and policies regarding the use of these accounts by the user, depending on the status of the user.

Using the system, an organization may provision, or allocate, services to a user within the organization based on defined policies, organizational information, attributes, and the role of the user in the organization. The policies, or rules, may be pre-defined for the organization based on the needs of the organization and incorporated into the system. The policies may be flexible enough to account for the various roles within the organization and the services each role requires. For example, assume an organization hires a new employee in the capacity of System Administrator. Using the system, several actions may be automatically initiated. For example, if a pre-set policy for the organization provides that each employee receives regular telephone service, a regular telephone, and an e-mail account, then upon the hiring of a new System Administrator, the system will automatically notify the appropriate parties to set up a regular telephone account and an e-mail account for the System Administrator and deliver a regular telephone to the System Administrator's office. Assume also that a pre-set policy for the organization is that each System Administrator has access to all system databases. The system will then automatically grant the System Administrator access to all system databases.

For purposes of illustration only, assume that the same organization hires a new employee in the capacity of Outside Salesperson. As before, because of the policies that have been pre-defined for the organization, including, but not limited to, the policy that each employee receives regular telephone service, a regular telephone, and an e-mail account, the system automatically notifies the appropriate parties to set up a regular telephone account and an e-mail account for the Outside Salesperson and deliver a regular telephone to the Outside Salesperson's office. However, if the organization has a pre-defined policy that Outside Salespersons do not have access to all system databases, as do System Administrators, then access to these databases may be automatically denied by the system to the Outside Salesperson. If, however, the organization has a pre-defined policy that all Outside Salespersons receive cellular telephones, then the system may automatically set up a cellular telephone account for and order delivery of a cellular telephone to the Outside Salesperson.

Preferred embodiments of the system described herein perform these actions automatically based on the role of the person within the organization and policies that are pre-defined for the organization. The policies may be based on the needs of the organization and the requirements of each particular role within the organization, such that resources may be provisioned to each user to meet the needs and the requirements of the user's particular role in the organization.

### System Logical Architecture

A logical architecture view of applications and modules of a system according to one embodiment of the present invention is shown in FIG. 3. As shown in FIG. 3, an example system embodiment may be characterized as a group of software modules with interfaces that allow the modules to collaborate with each other in order to implement the features of the system. In preferred embodiments, each module may be a self-contained unit of software that may be replaced within the system without compromising the integrity of the system, as long as the interface of the replaced module is maintained. While the interface to the module may remain consistent, the internal architecture of each module may vary, depending upon the application of use.

The modules may be grouped into an applications subsystem 102 and a platform subsystem 104. The applications subsystem 102 is directed toward applications that help a user or an administrator perform specific functions and, thus, may be implemented in software running on computers operated by users or administrators. The platform subsystem is directed toward services and utilities for enabling applications to interact with directories and databases containing the state of a network and the services on that network that are being managed. The platform subsystem may be implemented in software running on the platform computer system.

The applications subsystem 102 may include, for example, administration applications 106, application framework 108 and user applications 110. Administration applications 106 are applications used by an administrator, via the network, for various administration purposes. These applications may include one or more System Configuration applications 112, which provide an interface to allow an administrator to configure certain properties of the system. For example, the administrator interface may allow administrators to make system configuration settings, including, but not limited to, directory communication settings, logging properties, e-mail service settings, and garbage collection settings. The System Configuration applications 112 may include an interface to a Form Generation application 114, invoked to provide custom forms for data managed by the system. An example of such a form is illustrated in FIG. 8.

The Form Generation application 114 may also allow an administrator to create custom forms to be displayed in user and administrator applications. The Form Generation application may comprise a graphical user interface builder that associates system data attributes with graphical controls, which may include, but is not limited to, a "What You See Is What You Get" (WYSIWYG) graphical user interface builder.

The administration applications 106 may also include one or more Service Configuration applications 116, which provide an interface to allow administrators to configure certain properties of a service managed by the system. Examples of properties of a managed service include, but are not limited to, network location (IP address and port number), encryption for use and management, administrator login (ID and password), and management protocols.

In one preferred embodiment, a service may be bundled as a set with other services that are related through administrator-defined dependencies defined through the administrator interface. The Service Configuration applications 116 may include an interface to the Form Generation application 114 to provide custom forms for the account information to be used in the User Management web user application, which is the Web-based user interface that allows a user to add, modify, and delete other users.

The application framework 108 comprises a framework that integrates administrator and user applications. The application framework may include one or more System Browser applications 118, accessible by the system administrator, that preferably provide a graphical display of the entire managed contents of the system in a format that is easy to use.

The user applications 110 are applications used by an end-user, over the network, for various purposes. The user applications 110 may include one or more Organization Management applications 120 that preferably provide a graphical display of an organization's hierarchy of data in a format that is easy to use. From this interface, organizational units, locations, business partner organizations, users, system roles and organizational roles in the form of a tree view can be constructed and altered.

Depending upon the access level of the user, different areas of the hierarchy can be viewed or modified by the user. In embodiments in which the system manages multiple organizations, a user in a given organization will be restricted from accessing other organizations' data. However, a system administrator (not to be confused with an employee administrator or a customer administrator, described below) may be provided with access rights to all organizations' data.

The user applications 110 may include one or more Request Management applications 122 that provide an interface for the user to review and manage change requests pending within the system. A change request is a request to change one or more attributes of a user, or a request to change one or more attributes of a service belonging to that user. The interface may allow, for example, users acting in a supervisory role to approve or disapprove change requests.

The user applications 110 may also include one or more Form Viewer applications 124 that dynamically display forms as they are designed by the Form Generation administration application 114. The access level of the user determines which form, if any, the Form Viewer application will display in different situations. One or more Report Viewer applications 126 may be included for allowing a user to instruct a Report Engine in the platform subsystem 104 to execute predefined reports, and for displaying the results to the user. The access level of the user determines which reports the Report Viewer will provide. In addition, the user applications include applications for allowing a user to submit a request for provisioned services.

The user applications 110 may also include a Policy Management application 128 that provides an interface for defining policies that control the provisioning of services to users. In addition, constraints on individual attributes of services may be defined. The policies determine an association between the users and the services or resources, and constraints on those services provisioned to the users, based on attributes and user roles. The policies may define one or a series of approvals that are required before provisioning a given service or any service to a user. For example, such approvals may be required from one or more other users acting in a supervisory role. Policies may require one or more approvals if an attribute constraint is violated. The approvals may be defined using a Workflow Management application 130, which provides an interface for defining the approval process needed for a request in the system.

As described above, the platform subsystem 104 includes service and utility modules that enable various applications of the system to interact with directories and databases that hold information relating to the state of the system and services available over the network. The platform subsystem 104 may include, for example, application services 132, data services 134 and remote services 136. In preferred embodiments, the platform modules are designed to be as independent as possible of any domain-specific information. This enables the platform to be easily applied to a different domain and support a new set of applications without (or with minimal) re-architecture.

The application services 132 includes modules that may be used by several other system applications (client applications) to perform a service. These service modules

may provide a separate and independent set of capabilities to their client applications. The applications services modules 132 may include an Authorization module 138 for providing a set of authentication implementations that may be used by client applications. Such implementations may include, but are not limited to, simple password authentication techniques or X.509 certificate authentication.

The application services 132 may also include an Authorization module 140 that provides an interface for authorized users to define authorization rules, and enforces those rules as client applications attempt operations on the system, such as requesting services or data. These rules may apply to accessing data within the system, as well as to operations that can be applied to the system data, such as add, modify, or delete operations.

A Business-To-Business (B2B) Gateway module 142 may be included to provide an interface to an external access management system such as the RPM system described herein, or a comparable third-party system.

The B2B Gateway module 142 may provide an external system the ability to add, modify, delete and query user information. In preferred embodiments, these functions may be performed through an open protocol such as, but not limited to, secure hypertext transport protocol (HTTPS) to enable secure communications through the Internet. In preferred embodiments, requests made by external systems to carry out such functions may be stored in an RPM database or other storage facility 144 for auditing purposes.

The applications services 132 may also include a Logging module 146 that provides a utility for logging information, such as alarms and historical events, into persistent storage (e.g. the RPM database 144) associated with the platform system.

The applications services 132 may also include a Policy Engine 148 for executing policies that associate users with services. The Policy Engine 148 functions to determine whether or not provisioning requests conform to defined policies and to provide correct recovery procedures in the event that a policy is violated. If an approval is needed for a provisioning request, the Policy Engine 148 interfaces with a Workflow Engine 150 to notify and obtain authorization instructions from the appropriate authorization entity, which may be, for example, one or more users having pre-defined supervisory roles.

The Workflow Engine 150 functions to execute and track transactions within the system. Such transactions may include provisioning and de-provisioning of services, user status changes, and the approval process associated with a provisioning request in the system. In preferred embodiments, users with appropriate access levels may, through a client  
5 application, query the Workflow Engine for status information relating to a transaction (such as a provisioning request) being executed by the system.

The applications services modules also include a Report Engine 152 for executing predefined reports and formatting requested information. Note that requests for reports will only come directly from users of the system or the system administrator. They  
10 will not come from other systems.

The data services modules 136 includes modules that assist other modules in interacting with directories and databases that hold the network's state and the system's configuration. The data services modules 136 may include an Information Model 154 that provides a logical view of the data in persistent storage in a manner that is independent of the  
15 type of data source that holds the data. The model abstracts the details of the stored data into more usable constructs, such as Users, Groups and Services, by adding an object-oriented layer on top of the LDAP-based data model. The model may also provide an extendable interface to allow for customized attributes that correspond to these constructs.

The data services modules 136 may also include a Meta-Data module 156 that  
20 provides an interface from which a client may discover the design of the directory schema. Meta-Data is data that defines the content of the actual data. This may be used by a client to manage the data in persistent storage with a dynamic approach.

The remote services modules 134 provide interaction with external systems for provisioning and de-provisioning services. Synchronization of service information and user  
25 information, which is the process of making sure that the information stored on the remote service and the information stored in the RPM system match and is up to date, may also be performed by the remote services modules 134.

The remote services modules 134 may include a Message Transformation module 158 that provides utilities for defining and executing conversions of messages such as  
30 add, modify, delete, and search from one format to another. This module handles message

formats, rather than delivery protocols. The actual protocols used are determined at run-time, and may include, but are not limited to, Remote Access Management Protocol (RAMP), Encrypted Socket Protocol (ESP), and Directory Access Markup Language over HTTPS (DAML/HTTPS). The message transformation module 158 transforms between the data  
5 format used in the LDAP directory and the format used on the external system. Both formats are key value pairs, but the names of the keys must be mapped as part of the conversion process.

The remote services modules 134 may also include a Provisioning module 160 for providing an abstraction layer for provisioning products and services through external  
10 systems. The abstraction layer hides the protocol being used from the provisioning system. The specific protocols used to perform the provisioning, such as those described above, are preferably isolated from the client of the module. In preferred embodiments, new provisioning protocols may be added to the module without disrupting the module interface.

The remote services modules 134 also include a Synchronization module 162  
15 that retrieves service information from external systems to keep the service information stored by the system up to date. In addition, the Synchronization module 162 may retrieve organizational information, such as organizational unit and user information. The module is preferably pre-set or configured to define the data needed, how to retrieve it, where to store it and how often to perform retrievals. The module may also define rules for resolving conflicts  
20 between information retrieved from an external system and currently stored data.

### System Components

An example component view embodiment of the system is shown in FIG. 4, wherein logical applications and modules of FIG. 3 are organized into system components. A component is a self-contained and independent software entity that can be deployed onto  
25 computer and networking hardware separately from other components within the system. In the FIG. 4 embodiment, applications and modules are arranged to form an Application Server component 202, a B2B Server component 204, a Service Server component 206, a Synchronization Server component 208, a Web Server component 210 and a Workflow Server



component 212. Each of these components is arranged in one of two domains, a trusted domain 214 and a demilitarized zone (DMZ) domain 216, relative to an untrusted domain 218.

A DMZ is a computer network (or a single computer) that is protected from a company's internal network (the trusted domain), but is accessible from the internet. The  
5 DMZ domain 216 contains systems that are accessible from the internet, and can access the internal network (trusted domain). The DMZ domain 216 will not typically contain any sensitive data or critical systems. The DMZ domain 216 is created so that even if a hacker breaks into the DMZ, the hacker would still have to break into the internal network from the DMZ. Although every effort is made to protect the DMZ from hackers, a security breach in  
10 the DMZ should not result in the theft or corruption of data, or in the loss of a critical system. The trusted domain, which is the internal network, is considered much more sensitive. Any intrusion into the trusted domain is considered a serious breach of security.

The Application Server component 202 is composed of modules for supporting users interacting with the system, for example, through the Web Server component 210. The  
15 Application Server component 202 is coupled to the Web Server component 210 and the Workflow Server through secure connections, such as secure remote method invocation (RMI) connections. The Application Server component 202 includes the authentication, authorization, report engine and logging modules of the application services 132 and data services modules 136 shown in FIG. 3. In preferred embodiments, the Application Server  
20 component also executes logic for the presentation of the Application Services modules, so that the Web Server component may remain as simple as possible. This also provides a security boundary for the Application modules.

In preferred embodiments, each request to the Application Server (requests from users for provisioned services) is authenticated and authorized before it is executed. At  
25 this level, only proper system credentials may be sufficient for authentication, to determine whether a valid Web Server is making the request. However, by requiring authorization of the requesting user before any request is executed, the Web Server component may remain in an untrusted domain.

The B2B Server component 204 is composed of modules for providing an  
30 interface to external systems such as another provisioning system of the type described herein,

or other third-party provisioning systems that may communicate requests to the platform system.

In the illustrated embodiment, the B2B Server component 204 includes the B2B Gateway module 142 and an Authentication module (see reference character 138 in FIG. 3) for authenticating B2B requests. The interface may be provided using a secure network protocol, such as HTTPS, for encrypting data transfer and for authentication of requestors. In preferred embodiments, all requesters must be authenticated and authorized before requests can be fulfilled. The B2B Server component 204 is also coupled to the Workflow Server 212, preferably through a secure connection, such as a secure RMI connection.

The Service Server component 206 is composed of modules for providing an interface to managed resources 26 and 66, and services that issue unsolicited notices or asynchronous provisioning confirmations to the system. The Service Server component 206 may be connected to managed services resources 26 and 66, through, for example, a DAML/HTTPS connection. In addition, the Service Server component 206 may be connected to databases, such as a customer database 24, and third party service provider systems 28 and 64, through suitable connections, which may comprise HTTPS connections or vendor-specific connections.

The Service Server component 206 includes a Notification Gateway module which provides receiving logic that interacts with the Synchronization and Provisioning modules of the Synchronization Server 208 and the Workflow Server 212 components, respectively, through secure connections such as secure RMI connections. The separation of the Notification Gateway module from the Synchronization and Provisioning modules provides a security boundary between untrusted and trusted domains. The protocols used may be specific to the managed entity. In preferred embodiments, all requestors must be authenticated and authorized before passing on information to any modules in the trusted domain.

The Synchronization Server component 208 includes modules for periodically synchronizing service information between the service providers 28, 64 and a local data repository. The Synchronization Server component 208 is configured to adapt to the service provider's interfaces to extract desired information. The Synchronization Server component 208 includes the synchronization and message transformation modules of the remote services

134, the authentication, authorization, and logging modules of the applications services 132, and the data services modules 136 shown in FIG. 3.

The Web Server component 210 includes modules for providing users with a graphical interface. The Web Server component includes an Applications Presentation  
5 module, which creates Web pages for the end user, as well as the authentication module of the applications services module group 132. The Web Server component is connected to client systems 16, 52, for example, over an HTML/HTTPS connection. Preferably, all clients are authenticated when making requests to the system. For example, the Web Server may be configured to require password authentication, X.509 certificate authentication, or both, when  
10 using HTTPS.

The Workflow Server component 212 includes modules for provisioning and de-provisioning services within the system. The Workflow Server component includes the policy engine, workflow engine, logging, email, authentication and authorization modules of the applications services module group 132, as well as the data services modules 136 and the  
15 provisioning and message transforming modules of the remote services module group 134.

### Deployment of System Components

The components 202-212 of the FIG. 4 embodiment may be deployed in hardware (processor or computer systems) in a variety of manners. The components may be deployed on as few processors as possible, for example, to minimize system complexity and  
20 operational cost. Alternatively, some or all of the components may be separated and distributed to separate processors to maximize computing resources. Many of the modules and applications within components can also be distributed to further maximize computing capabilities. Furthermore, some or all of the components may be configured in clusters to take advantage of load balancing algorithms and fail-over capabilities.

25 The responsibility of configuring the system deployment may be provided to a system administrator. Thus, applications, modules or components containing groups of applications or modules as described above may be provided to a system administrator, for example, in software form (such as on a computer readable storage medium), in hardware or firmware form (such as on circuit boards or cards to be installed in a computer system) or a

combination thereof. The system administrator may then develop a deployment strategy that meets the organization's performance and security needs and deploy the appropriate modules on appropriate hardware devices to fit the desired strategy. The system administrator may be free to deploy all of the components of the system on one processor or distribute clusters of  
5 each component in almost any combination, if desired.

An example of simple deployment option is shown in FIG. 5, where the six components 202-212 of FIG. 4 are clustered onto one processor 302 comprising the Platform system. Thus, processor 302 represents a server running the provisioning system according to embodiments of the present invention described herein. The Platform Processor 302 is  
10 coupled to external systems and clients over the network 306, through a Web Server Load Balancer 308. One or more Data Server processors 304 may be coupled to the platform processor 302 for deploying the RPM Directory and RPM Database. The Data Server processors 304 include a server running a relational database server and an LDAP directory server. The FIG. 5 embodiment demonstrates a simple deployment with a clustered  
15 deployment of servers that deploy all the components of the system. The load balancing algorithms dictate which components are running on specific processors. This deployment embodiment, however, may present security risks because the components are not deployed on separate hardware in separate trusted domains, as described above.

Another example of a deployment option is shown in FIG. 6. The FIG. 6  
20 deployment, while more complex than the deployment shown in FIG. 5, alleviates some of the security concerns associated with the FIG. 5 deployment. All components 210, 204 and 206 shown in the DMZ domain in FIG. 4 that interface to external clients and systems via the Internet may be clustered on one or more dedicated Web Server processors 402 in FIG. 6 to create a boundary between untrusted and trusted domains, where the web client is in an  
25 untrusted domain and the rest of the system components are in a trusted domain. The Synchronization Server component 208 is deployed in a separate cluster, so that communication with the service providers can be configured independently of other clusters.

In this manner, the interfaces to external clients and systems are isolated to one or more servers containing only those components of the system necessary for external  
30 interface. Other components of the system, including, but not limited to, those components

5

## 10

15

20

25

015.472852.3

A System Administration functional area may group all requirements for configuring the system. This may include requirements for installing the system and altering its configuration parameters. A User Interface Customization functional area may group all requirements for providing a user the ability to customize a user interface. A User  
5 Management functional area may group all requirements for adding, modifying, and deleting users.

Other functional areas may be developed based on the needs of the system user.

### System Operation

Examples of certain operations of the system are shown in the sequence  
10 diagrams of FIGS. 7A-E. FIG. 7A is a sequence diagram of interactions for implementing a user's authentication to the system. At the conclusion of the authentication, the user is presented with an application interface to perform system actions. In the illustrated embodiment, the user is presented an interface to an Organization Management application. FIG. 7B is a sequence diagram of interactions for adding a user to the system. FIG. 7C is a  
15 sequence diagram of interactions for implementing on-demand provisioning of a service for a user. FIG. 7D is a sequence diagram of interactions for synchronizing service data with a remote host and enforcing any policies that are violated by detecting changes made on the remote host.

FIG. 7E is a sequence diagram of interactions for implementing an addition of a  
20 user to the system and provisioning of services for that user based on provisioning policies. In embodiments of the present invention, user provisioning is accomplished with the RPM system described hereinabove. Unlike RBAC, which provisions users with "soft" resources (such as accounts) based on only on roles, RPM provisions users with both "hard" and "soft" resources based on policies, which are defined according to user roles and attributes.

25 Thus, in preferred embodiments of the present invention, the RPM system may provision a user with "soft" resources, including, but not limited to passwords, e-mail and voice mail accounts, application programs, databases, files, folders, the Internet, Web pages, organizational Intranets, and the like. Other, more non-traditional "soft" resources may include messages to third parties, digital certificates for enabling the user to access encrypted

resources, the capability to order products over the Internet, the ability to order a corporate credit card, access to financial services providers, and the like. In addition, RPM may provision users with "hard" resources such as telephones, computers, cellular telephones, pagers, personal digital assistants, desks, chairs, file cabinets, and other physical components.

5 RPM may also provide resource bundles, which are pre-packaged groupings of resources that are typically provisioned together. For example, a resource bundle may include a cellular telephone, telephone service, a pager account, voice mail, and Internet access. Another example of a bundled account may be Digital Subscriber Line (DSL) access and an Internet Service Provider (ISP) account.

10 Note that RPM systems according to embodiments of the present invention may also have the capability of making provisioning adjustments if a user's roles and attributes change, including de-provisioning, and especially de-provisioning all of the allocated resources once a user has left the company.

15 In preferred embodiments of the present invention, the RPM system provisions users with resources based on policies, which are defined based on roles and attributes. A role describes a person's responsibility within the organization, and may include roles such as a manager, secretary, system administrator, committee member, and the like. Each role has only two values. For example, a user is either a manager (a "yes" value), or he is not (a "no" value). An attribute is a characteristic or quality of a user or resource, such as "amount of  
20 time spent traveling," or "cost." In contrast to a role, each attribute may have multiple values. For example, the attribute "amount of time spent traveling" may have the values "less than 30%," "between 30% and 60%," and "greater than 60%."

Policies are written based on these roles and attributes. Because attributes can be used in addition to roles to define a policy, the task of defining the relationship between  
25 users and resources is made more efficient. Attributes can take on multiple values, and thus a single policy definition can be written in Boolean form using IF-THEN-ELSE IF statements (or the equivalent) to account for different attribute values, instead of multiple role definitions using IF-THEN statements. It should be noted that although IF-THEN-ELSE statements are presented herein for purposes of explanation only, in embodiments of the present invention  
30 any programming language and syntax capable of implementing the equivalent Boolean

statements may be employed. A simple example is illustrative. Suppose that a role-based system has defined three roles as follows:

Role No.	Definition
1	IF the user is in marketing AND the user is a manager AND the user travels less than 30% of the time, THEN provision the user with a pager;
2	IF the user is in marketing AND the user is a manager AND the user travels between 30% and 60% of the time, THEN provision the user with a cellular telephone;
3	IF the user is in marketing, THEN provision the user with access to the sales figures database;

5 Now suppose that a new employee, user A, is a marketing manager that travels less than 30% of the time. Suppose also that a new employee, user B, is a marketing manager that travels between 30% and 60% of the time. The role-based system would determine that roles 1 and 3 apply to user A, and that user A should be provisioned with a pager and access to the sales figures database. The role-based system would also determine that roles 2 and 3  
10 apply to user B, and that user B should be provisioned with a cellular telephone and access to the sales figures database.

Now suppose that a policy-based system according to embodiments of the present invention has defined two policies as follows:



Policy No.	Definition
1	IF the user is in marketing AND the user is a manager, THEN IF the user travels less than 30% of the time, THEN provision the user with a pager; ELSE IF the user travels between 30% and 60% of the time, THEN provision the user with a cellular telephone;
2	IF the user is in marketing, THEN provision the user with access to the sales figures database;

The policy-based system would determine that roles 1 and 2 apply to user A, and that user A should be provisioned with a pager and access to the sales figures database.

The policy-based system would also determine that roles 1 and 2 apply to user B, and that user B should be provisioned with a cellular telephone and access to the sales figures database.

It should be understood from the above example that embodiments of the present invention allow a single policy to be defined than covers multiple attribute values, minimizing the number of policies that need to be defined as compared to the number of roles that would have to be defined in a role-based system. In the simple example provided above, policy 1 of the policy-based system replaces roles 1 and 2 of the role-based system. With fewer policies to evaluate, less memory may be consumed. In addition, in preferred embodiments the determination of resources can be performed more quickly. In the simple example provided above, when user A is being evaluated, both IF-THEN statements in roles 1 and 2 must be evaluated before the role-based system can determine that role 1 applies to user A, but role 2 does not. In contrast, once the "IF the user travels less than 30% of the time" statement in policy 1 is found to be true, the ELSE IF statement in policy 1 can be bypassed.

The roles and attributes associated with a user, as described above, may be assigned by human resources personnel or other organizational employees prior to the user's start date. In preferred embodiments of the present invention, the provisioning of a user may be initiated by calling up a provisioning user interface (screen) on a Web browser connected to an organizational network. This screen would enable human resources personnel to input known roles and attributes. The RPM system would then search its stored policies and, based

on the user's roles and attributes, determine a set of resources to be provisioned.

Alternatively, human resources personnel may simply type employee information into a human resources (HR) system database, where the RPM system would automatically pull information from this database through a direct feed and begin the provisioning process. In addition, a  
5 start date or other date and time information may be entered, and the RPM system can initiate provisioning tasks when triggered by this date and time information.

The actual provisioning of resources may involve electronic communications and human interaction. For example, an e-mail might be sent to various office personnel to deliver a desk and chair to a certain office by a certain date. Another e-mail might be sent to  
10 IT personnel to deliver a computer and telephone to the office by a later date, and then enable a computer account, provide access to various applications and databases, e-mail, and voice mail by yet another date. Outside procurement services companies may also be contacted for some or all of the provisioning tasks. In addition, the provisioning of accounts maintained by an external system such as an ASP may be facilitated by communications between the RPM  
15 system and "agent" software that resides in a server within the external system. The "agent" acts as a portal through which accounts from the external system may be managed and accessed.

Once a user is provisioned with a set of resources, a list of these existing resources is maintained by the RPM system. Thereafter, if a user's roles or attributes should  
20 change, the policies are re-evaluated and a new list of resources to be provisioned are determined. This new list of resources is compared to the list of existing resources, and users are provisioned or de-provisioned according to the differences in the lists. In preferred embodiments, if a particular existing resource is also in the new list of resources, the RPM system will make no change regarding this resource, rather than de-provisioning then  
25 provisioning the resource.

Upon termination or suspension of a user, or if a user should take a leave of absence, embodiments of the present invention may also suspend the provisioning of resources, rather than de-provisioning them. For example, if a terminated user has threatened to take legal action against the company, the user's e-mail account may be suspended but not

deleted, so that the user cannot access the e-mail account, but the e-mails may nevertheless be reviewed by the company in anticipation of litigation.

In preferred embodiments of the present invention, a reconciliation process is performed when the RPM system is first invoked. In reconciliation, the RPM system  
5 compares a list of currently provisioned resources with a list of resources that should have been provisioned based on the current state of each user's roles and attributes. Discrepancies between the two lists are resolved by provisioning or de-provisioning.

Although the previous example described an attribute of a user ("amount of time spent traveling"), in embodiments of the present invention the RPM system may also  
10 maintain attributes of resources. Resource attributes play a role where the provisioning process allows for a selection of resources. For example, once a user begins working at an organization, the user may be able to call up the provisioning user interface screen to request optional resources. After entering additional information, the user may be able to select optional resources, provided that the user has certain attribute values.

Continuing the present example for purposes of illustration only, suppose that  
15 user A (a marketing manager that travels less than 30% of the time, and is not automatically entitled to a cellular telephone) can nevertheless request a cellular telephone if certain other roles and attributes are satisfied. User A may call up the provisioning screen and enter a value of "Europe" for the attribute "client location." The provisioning screen may then present user  
20 A with a selection of cellular telephones to choose from. If user A selects a cellular telephone less than \$200, a "cellular telephone cost" attribute having a value "less than \$200" will be associated with user A, and the system may automatically provision user A with that telephone by sending an e-mail order to a cellular telephone provider, for example.

However, if the selected telephone is more than \$200, such as a so-called  
25 "world phone," a "cellular telephone cost" attribute having a value "more than \$200" will be associated with user A, and approval may be required. For example, an e-mail may be sent to a vice-president, providing the vice-president with access to the provisioning screen and requesting that the vice-president input the approval or disapproval of the telephone. Once this information is provided, the RPM will either order the telephone or send a denial message to  
30 the user. An example policy definition covering this example is as follows:

Policy No.	Definition
1	<p>IF the user is in marketing AND the user is a manager, THEN</p> <p>IF the user travels less than 30% of the time, THEN</p> <p>provision the user with a pager;</p> <p>IF the user's client's location is in Europe, THEN</p> <p>IF the cellular telephone is less than \$200</p> <p>Provision the user with the cellular telephone;</p> <p>ELSE</p> <p>approval from a vice-president is needed to provision the user</p> <p>with</p> <p>the cellular telephone;</p> <p>ELSE IF the user travels between 30% and 60% of the time, THEN</p> <p>provision the user with a cellular telephone;</p>

Other examples of resource attributes include, but are not limited to, color, features, and manufacturer.

- 5 As described above, embodiments of the present invention may require input from another person before provisioning can continue. In another example provided for purposes of illustration only, when a new employee is entered into the system, human resources personnel may enter known roles and attributes, such as the new employee's department, at which time the policy may halt the inputting of information into the
- 10 provisioning screen and instead send an e-mail to the department manager, providing the department manager with access to the provisioning screen and requesting that the department manager input a cubicle or office location. Once this information is provided, human resources personnel are notified, and provisioning of that office with a desk, chair, etc. can resume. More generally, at any point in the provisioning sequence, the policy may require
- 15 that another person provide some of the new employee's roles, attributes, job descriptions, etc. before provisioning can resume.

It should be understood that although the above examples describe e-mail as a means for seeking information or approval from another person, or ordering resources, other methods of communication such as providing hyperlinks to Web pages and automated ordering of resources over the Internet using online resource provider order sheets may also be employed.

As described above, in embodiments of the present invention the provisioning process may be a sequence of steps, some of which require human intervention such as providing information or authorization. An example of this sequence will now be provided. Referring to FIG. 7, a user wishing to be provisioned with one or more resources may access a provisioning user interface screen 700 from a networked computer. In embodiments of the present invention, the provisioning screen 700 may include explanatory text and boxes or fields into which information may be entered. The user may type information into the fields, or may select from a pulldown menu of fixed choices. For example, fields 702 and 704 for a user to enter his first and last name may be provided, and a pulldown menu 706 of available resources may be provided. In alternative embodiments, the provisioning screen 700 may also include fields for optional information, fields for required information that the requesting user does not know (and therefore must be provided by another person), fields for required information (such as approvals) that must be provided by another person, and the like. In preferred embodiments, however, the provisioning screen visible to the requesting user will only contain those fields for information that the user is capable of providing.

Continuing the example of FIG. 7 for purposes of illustration only, suppose that the user requests an e-mail account. In embodiments of the present invention, the RPM processes the provisioning request by sending the provisioning screen to the manager, sending an e-mail to the manager to access a particular hyperlink to view the provisioning screen, or the like. As indicated by reference character 708, the department manager may see a different provisioning screen 708 from the requesting user. For example, the provisioning screen 708 may include additional fields 710 and 712 which allows the manager to approve or disapprove the request, and, if approval is given, which department has given the approval.

Continuing the example of FIG. 7 for purposes of illustration only, if approval is given, the provisioning screen may then be made known to the IT department, who may see

a different provisioning screen 714 from the department manager. For example, the provisioning screen 714 may include an additional field 716 which allows IT personnel to designate a particular mail server, which may be dependent on the department information, and which may be beyond the department manager's knowledge.

5 As the preceding example illustrates, in preferred embodiments of the present invention, software for controlling the optional provisioning process may establish which information is to be provided by an individual, and which individuals have approval or disapproval authority, etc. The provisioning process may also determine who can modify information, and which information cannot be modified. The provisioning process may also  
10 define what information must be added before the provisioning request can be sent to the next person. In alternative embodiments, the provisioning request may be sent back to the requesting user for additional information or the modification of existing information (i.e. the modification of a resource request). In preferred embodiments, the authorizing authority may change depending on what is entered into the request fields. Thus, there is no one process  
15 path through which this request form will flow. The process path may actually branch into different directions, depending on what information is entered into the fields of the request form. A generic name for this flow is called workflow process.

#### **System Operation Using a Third Party as an RPM Service Provider**

20 An embodiment of the invention as described up to this point may be shown very generally in FIG. 9. A first organization 800 provisions resources (not shown) using a first server 802 by interfacing with such resources through the first organization's agents 804. Independently, a second organization 806 provisions resources (also not shown) using a second server 808 by interfacing with such resources through the second organization's agents 810.  
25 Note that in this configuration, two logical servers, and possibly even more physical servers, are being utilized by two independent vendors for the same purpose. Although this configuration is typical and may be necessary, it may also be redundant in a variety of circumstances.

30 An alternative embodiment of the present invention is shown in FIG. 10. Here, a first organization 800 also provisions resources; however, rather than provisioning resources

using a server under its, the first organization 800 may have its resources provisioned by a third party RPM service provider operating a third party server 820. The first organization 800 may interface with the third party server 820 through a network 822, such as, for example, the Internet. Likewise, the third party RPM service provider may interface with the first organization's agents 804 through the network 822 to provision resources for the first organization 800. Likewise, the second organization 806 may have its resources provisioned by the third party RPM service provider using the third party server 820 through the network 822. The third party RPM service provider may interface with the second organization's agents 810 through the network 822 to provision resources for the second organization 806. Thus, in this embodiment, both organizations 800, 806 utilize a single logical server 820 operated and controlled by the third party RPM service provider.

According to this embodiment of the invention, both organizations may take advantage of the efficiency of a single logical third party server 820 operated by a third party over a network 822, thereby removing the costs associated with purchasing and operating a server for resource provisioning activities. Also, the third party RPM service provider may function as a data center and provide resource provisioning as a managed service to the organizations 800, 806, whereby the organizations 800, 806 may become customers of the third party RPM service provider. The managed service may be provided on a subscription basis, whereby any organization desirous of such services may pay a set periodic fee for all of its resource provisioning needs.

For example, assume it is the policy of a first company to provide its salespersons with an email account and access to its customer database. Assume also that this first company has chosen to outsource its resource provisioning requirements to a trusted third party RPM service provider. Assume also that it is the policy of a second company to provide all its employees with an account on its networking operating system, and that the second company has also chosen to outsource its resource provisioning requirements to a trusted third party RPM service provider. Both companies would provide the trusted third party RPM service provider with relevant employee information and the nature of the access rights to be granted to the salespersons of the first company and the employees of the second company.

Such information could be provided by both companies to the trusted third party RPM service provider over a network such as, for example, the Internet.

The trusted third party RPM service provider may maintain such information on its server or servers. This would allow the trusted third party RPM service provider to  
5 immediately provision a new salesperson or new employee with the required resources. All that would be required to effect such provisioning would be that each company provide the trusted third party RPM service provider with relevant changes to salesperson or employee information. Based on such changes, the trusted third party RPM service provider could create, change or remove accounts or otherwise modify provisioning on required resources.  
10 Alternatively, each company could provide the trusted third party RPM service provider with the exact nature of the provisioning change required.

A flowchart detailing a method for implementing the embodiment of FIG. 10 is shown in FIG. 11A. A request for provisioning services is received by a third party RPM service provider at step 830. Such a request may be made by one or more companies needing  
15 such services. The request may be made via electronic means or by personal contact between the appropriate persons at the company and at the third party RPM service provider.

At step 834, the third party RPM service provider receives user information from the company making the request. This information may include, but is not limited to, user name, user number, a list of resources to which the user will have access, the nature of  
20 the access rights, and the like. This information may be sent electronically from the customer to the third party RPM service provider using a network, such as, for example, the Internet. The third party RPM service provider will also receive notification that the user is authorized to access the appropriate resources from the customer at step 836. This information may also be sent electronically from the customer to the third party RPM service provider using a  
25 network, such as, for example, the Internet.

At step 838, the third party RPM service provider provisions the relevant resource or resources for the user via agents. It should be noted that many systems may be provisioned at this step to effect the required provisioning. Such provisioning may also take place over a network. Once the resource or resources have been provisioned for the user, the  
30 user is notified accordingly at step 839 and is then at liberty to utilize the resource or resources



in accordance with the provisioning policy established by her employer. This process may be repeated as many times as necessary for each company making a request to the third party RPM service provider for provisioning of its resources.

A flowchart detailing an alternative method for implementing the embodiment of FIG. 10 is shown in FIG. 11B. A change in user information is received by a third party RPM service provider at step 831. The changes may be received via electronic means over a network, such as, for example, the Internet, or by personal contact between the appropriate persons at the company and at the third party RPM service provider and may include, without limitation, changes in user name, user role, user organization, user title, user location, and the like. Also, such changes may be received automatically. For example, a mechanism may be implemented whereby any changes made to a company's human resources database are automatically sent to or retrieved by the third party RPM service provider.

At step 832, the third party RPM service provider determines which changes in resource access rights are needed based on the user information changes received. This may be done independently of the company sending changes in user information. At step 833, the third party RPM service provider obtains any approvals necessary for provisioning changes prior to effecting such provisioning.

At step 835, once the necessary approvals have been received, if any, the third party RPM service provider provisions, which may include, without limitation, deprovisioning, the relevant resource or resources for the user via agents. It should be noted that many systems may be provisioned at this step to effect the required provisioning. Also, resources may be provisioned in parallel. Such provisioning may also take place over a network. Once the resource or resources have been provisioned for the user, the user is notified accordingly at step 837 and is then at liberty to utilize the resource or resources in accordance with the provisioning policy established by her employer.

In the embodiment of the invention shown in FIG. 10, the resources being provisioned may all be contained within a customer's "information technology" space. That is, the resources being provisioned may not necessarily exist at the customer's site, but may be within the realm and under the control of the customer. For example, these types of resources

may include, but are not limited to, email, operating systems and databases. Such resources may exist worldwide, but, nonetheless, may still be within the control of the customer.

An enhancement to the embodiment of FIG. 10 is shown in FIG. 12. In this embodiment, resources 840 external to the first organization 800 and the second organization  
5 806 may be accessed and utilized by both organizations 800, 806 through a network 822 and provisioned for both organizations 800, 806 by a third party RPM service provider using a third party server 820. The third party RPM service provider and the organizations 800, 806 may interface with these resources 840 via agents.

For example, continuing with the example used in reference to FIG. 10, assume  
10 the first company and the second company provide all of their management level employees with a charge card account, such as, for example, an AMERICAN EXPRESS card. Assume also that both companies have also chosen to outsource its provisioning requirements for this resource to a trusted third party RPM service provider. Both companies would provide the trusted third party RPM service provider with relevant employee information, such as, for  
15 example, the names of employees who have management positions within their respective companies, the employee numbers of such employees, the charging authority granted to each individual employee, and the like. Such information may be provided by both companies to the trusted third party RPM service provider over a network such as, for example, the Internet.

20 The trusted third party RPM service provider would then establish the appropriate relationship with the charge card company such that the trusted third party RPM service provider would have the requisite authority to establish accounts on behalf of the companies and provision employees of both companies with charge cards for such accounts through agents. Once the relationships between the companies and the trusted third party  
25 RPM service provider, the companies and the charge card company, and the trusted third party RPM service provider and the charge card company have been established, the provisioning of employees at any of the companies with a charge card account may be immediate. All that is necessary is that a company notify the trusted third party RPM service provider of its provisioning requirement and supply the trusted third party RPM service  
30 provider with the necessary employee information. The trusted third party RPM service

provider can then establish the account with the charge card company and instruct the charge card company to forward one or more charge cards to the employee of the company for whom the account is being established.

Another alternative embodiment of the present invention is shown in FIG. 13.

5 In this embodiment, any number of companies 800, 806 may use a third party RPM service provider for provisioning resources through agents 804, 810. These companies 800, 806 may utilize their own resources and have these resources provisioned through a network 822, such as, for example, the Internet, by the third party RPM service provider using a third party server 820. However, these companies 800, 806 may also be considered vendors of their  
10 respective resources and may choose to affiliate themselves with one another and share resources. This is easily facilitated due to the third party RPM service provider being a common and trusted link to each vendor. Thus, the resources owned and operated by each affiliate organization may be "cross-provisioned" among the affiliated organizations by the third party RPM service provider. This embodiment of the invention may also be described as  
15 a "resource exchange."

Also, according to this embodiment of the invention, the infrastructure may be considered semi-private because, although it is not completely private as the enterprise and ASP embodiments described previously are, it is also not completely open to the public. The infrastructure, and, consequently, the resources available within the infrastructure, may be  
20 open only to those vendors of resources who have chosen to affiliate themselves with other vendors utilizing a third party RPM service provider for purposes of having such resources provisioned by such a service provider.

As an example of the embodiment of the invention shown in FIG. 13, suppose that a first vendor belonging to a resource exchange, i.e., belonging to a provisioning  
25 infrastructure, has the capability to provide email systems for other organizations. Suppose also that a second vendor in the same resource exchange provides database access to various consumer lists. Suppose also that the first vendor determines it has a need for various consumer lists and decides it would like to obtain the database information controlled by the second vendor. Finally, suppose that the second vendor determines it would like to implement  
30 an email system for its employees. Then, upon notification by each company to the third party

RPM service provider, the third party RPM service provider may cross-provision the first vendor with the database resource belonging to the second vendor. Likewise, the third party RPM service provider may cross-provision the second vendor with the email system provided by the first vendor. In this type of cross-provisioning embodiment and others, because the third party RPM service provider is a trusted authority, it may mask the identity of the an employee or employees, which may be original or true identities, by provisioning a “pseudo-account” for the second vendor.

Because both vendors are members of the resource exchange, most, if not all, of the information required by the third party RPM service provider for cross-provisioning of the resources for each vendor will already be available to the third party RPM service provider. In addition, both vendors will typically have entered into an agreement regarding the cross-provisioning of resources, such agreement generally being a condition precedent to becoming a member of the resource exchange, the details governing such cross-provisioning will already have been put in place. Thus, the provisioning of the desired resources may be immediate once the request for provisioning is made.

As another example of the embodiment of the invention shown in FIG. 13, suppose that an organization in a resource exchange contracts with a charge card company providing that every vice-president in the organization be given access to one of the charge card company’s charge accounts. Assuming that the charge card company is also a member of the resource exchange, as soon as the contract is effective, each vice-president in the organization may immediately and automatically be provisioned by the third party RPM service provider, through the resource exchange, with a charge card company charge accounts. There need be no additional flow of individual information to effectuate the provisioning. All information required for the provisioning of the organization’s vice-presidents with charge accounts will already be available on the system, since both the organization and the charge card company will have already been members of the exchange. However, if desired, additional approval processes may be executed prior to any such provisioning.

Also, the provisioning may be done in the aggregate. Because the organization will have already identified to the third party RPM service provider its policies for the roles

and attributes of persons within its organization, such as those policies applicable to vice-presidents, and because the charge card company will have already identified to the third party RPM service provider its policies for anyone who needs to be provisioned with one of its charge accounts, the third party RPM service provider can coordinate the requirements of both organizations and expeditiously provision the vice-presidents with charge accounts.

For example, the organization might have a policy that says vice-presidents get an annual spending limit of \$100,000. The charge account might be set, then, to limit annual purchases for vice-presidents to \$100,000. Also, the organization might have a policy that says any single purchase by a vice-president cannot be greater than \$10,000 without approval from the president. Thus, the charge account might be set, then, with a single purchase limit for vice-presidents of \$10,000. So, once a role and its attributes have been established in the system, it can immediately be adapted to the provisioning of a resource without further effort by the organization.

In this embodiment, a user can also be de-provisioned very quickly. For example, assume a vice-president in the organization is terminated or leaves the organization. Although her paychecks may stop immediately, her charge account could typically remain open until the end of the month. This could be very dangerous for the organization in that the vice-president may still have purchasing power on the charge account even though she is no longer affiliated with the organization. In this embodiment, if the organization tells the third party RPM service provider that the vice-president is no longer with the organization, the third party RPM service provider can immediately de-provision the vice-president from her charge card account, thereby protecting the organization from unauthorized usage.

A flowchart detailing a method for implementing the embodiment of FIG. 13 is shown in FIG. 14A. A request for provisioning services is received by a third party RPM service provider at step 850. Such a request may be made by one or more companies needing such services. The request may be made via electronic means or by personal contact between the appropriate persons at the company and at the third party RPM service provider.

However, in this embodiment the provision request is made for a resource not owned or operated by the company making the request. For example, a company might make a request for email provisioning, but, in actuality, the company might not have an email resource.

Accordingly, the company would be looking to an affiliate within the resource exchange to provide email services, and would be looking to the third party RPM service provider to provision such services.

At step 854, the third party RPM service provider provisions appropriate  
5 resources within the resource exchange for the company making the provisioning request. Once provisioning is complete, the user is notified accordingly at step 856 and is then at liberty to use the resource according to the provisioning policy of the company and in accordance with an agreement between the company requesting the provisioning of the resource and the company providing the resource for provisioning. Typically, such an  
10 agreement would be a condition precedent to becoming a member of the exchange.

A flowchart detailing an alternative method for implementing the embodiment of FIG. 13 is shown in FIG. 14B. A change in user information is received by a third party RPM service provider at step 851. Such changes may be received by one or more companies having such changes. The changes may be received via electronic means or by personal  
15 contact between the appropriate persons at the company and at the third party RPM service provider. Also, such changes may be received automatically. For example, a mechanism may be implemented whereby any changes made to a company's human resources database are automatically sent to or retrieved by the third party RPM service provider.

Also, in this embodiment the changes may be for users who are provisioned for  
20 a resource or resources not owned or operated by the company by whom the user is employed. For example, a company might have a change for a user with respect to email, but, in actuality, the company might not have an email resource. Accordingly, the company would be looking to an affiliate within the resource exchange to provide its email services.

At step 852, the third party RPM service provider determines which changes in  
25 resource access rights are needed based on the user information changes received. This may be done independently of the company sending changes in user information. At step 853, the third party RPM service provider obtains any approvals necessary for provisioning changes prior to effecting such provisioning.

At step 855, the third party RPM service provider provisions, which may  
30 include, without limitation, deprovisioning, appropriate resources within the resource

exchange for the company providing changes in user information. Provisioning of multiple resources may be done in parallel. Once provisioning is complete, the user is notified accordingly at step 857 and is then at liberty to use the resource or resources according to the provisioning policy of the company and in accordance with an agreement between the company requesting the provisioning of the resource and the company providing the resource for provisioning. Typically, such an agreement would be a condition precedent to becoming a member of the exchange.

Billing for cross-provisioning services among affiliates may take a variety of forms. For example, a transaction fee may be applied by a vendor each time a resource is provisioned. Such fee may be payable to the customer requesting provisioning to the vendor of the resource, with a percentage of such fee payable to the third party RPM service provider. Alternatively, a subscription may be paid by a customer requesting provisioning to the vendor of a resource such that all provisioning fees are included in the subscription rate. This type of billing arrangement may be attractive to a customer with heavy provisioning needs if such needs can be anticipated.

Various techniques to facilitate the cross-provisioning of resources among affiliates may be included, without limitation, in the embodiment shown in FIG. 13. For example, to facilitate cross-provisioning of resources in a resource exchange, a "footprint" of the roles and attributes within each affiliate organization in the exchange may be made generic. That is, each role within one affiliate organization may translate to a corresponding role in another affiliate organization. This may be made possible by a translational map that translates roles from one affiliate into another. For example, a sales engineer in one affiliate may be referred to as a technical sales consultant in another affiliate. Even though these two positions may be identified differently in their respective organizations, the duties required by the positions may be the same in the context of the exchange. Thus, the third party RPM service provider may maintain a translational map that coordinates the access rights and entitlements of these two positions between affiliate resources. So, a sales engineer in a first affiliate may have the same entitlement to resources as a technical sales consultant in a second affiliate and vice versa. The third party RPM service provider may provide a mapping to standard affiliate organizational footprints or standard policies.

Another technique used to facilitate the cross-provisioning of resources among affiliates in the embodiment shown in FIG. 13 relates to high level authentication of affiliates. Success of an affiliate resource exchange may require that each affiliate be authenticated with respect to various business and financial aspects of such affiliates, including, without  
5 limitation, background checks, credit worthiness checks, cash flow checks, and other aspects of an affiliate's business and financial viability. Such high level authentication may be performed by the third party RPM service provider and used in addition to an authentication of identity provided by various techniques including, but not limited to, passwords and multifactor approaches such as PKI and biometrics.

10 Yet another technique used to facilitate the cross-provisioning of resources among affiliates in the embodiment shown in FIG. 13 relates to identity synchronization. In order for cross-provisioning of resources to function smoothly in a resource exchange, updated information regarding resource users and affiliates within the exchange must be readily available. For example, should an affiliate leave the exchange, this must be reflected as soon  
15 as possible within the list of resource exchange affiliates so that other affiliates may plan and take action accordingly, especially if the departure of an individual means exposure to loss for a critical resource of another affiliate. Conversely, should an organization providing a valuable resource or resources become a member of the exchange, such information should also be made available to other affiliates of the exchange so that they may readily take  
20 advantage of the additional resource or resources available. Such a resource or resources may be registered in the exchange and provisioned accordingly by the third party RPM service provider.

A third party RPM service provider may provide such identity synchronization within the resource exchange. Such synchronization is made possible from a practical  
25 standpoint due to the fact that the third party RPM service provider may function as a data center for all affiliate members of the resource exchange. Thus, all information required to update resource exchange information is available on one logical server and updates can, therefore, be made quickly and efficiently.

Yet another technique used to facilitate the cross-provisioning of resources  
30 among affiliates in the embodiment shown in FIG. 13 relates to audit trails. It may be



advantageous for security, accountability and other reasons for each affiliate of the resource exchange to have a record of each cross-provisioning transaction completed for its own resources by the third party RPM service provider. Moreover, it may also be advantageous for each affiliate of the exchange to have a record of each cross-provisioning transaction completed for its users of another affiliate's resources. A third party RPM service provider may provide an audit trail, i.e., a record of each provisioning transaction, for affiliates of the resource exchange. Such an audit trail may be implemented by a third party RPM service provider since, as before, a third party RPM service provider may function as a data center for all affiliate members of the resource exchange. Thus, all information regarding provisioning transactions may be easily recorded and provided to affiliate members at their request.

Yet another technique used to facilitate the cross-provisioning of resources among affiliates in the embodiment shown in FIG. 13 relates to anonymity of individuals and organizations interacting with resources. In the event resource usage within a resource exchange is subject to interaction, such as, for example, bidding, identities of the affiliates involved in such interaction may be made anonymous during the interaction process. That is, during such interaction, affiliate identities may be masked out so that the interaction process is not skewed by the identity of the affiliates.

There may be three levels of anonymity implemented in a resource exchange. First, there may be no anonymity at all. Using bidding as an example, it may be unimportant to the affiliates that their identities remain anonymous during a bidding process. Consequently, their identities may be made known to the other affiliates bidding on a resource. Second, the identities of affiliates bidding on a resource may be masked out, but a user doing the actual bidding may be assigned some type of unique identifier to be used for all bidding sessions. Third, the identities of affiliates bidding on a resource may be masked out and a generic identifier used for only one bidding session may be assigned to a user doing the actual bidding; at subsequent bidding sessions, a different generic identifier may be assigned to the same user doing the actual bidding. Such anonymity may be facilitated by a third party RPM service provider since a third party RPM service provider functions as a centralized provider of provisioning services for all affiliate members of the resource exchange. Thus, identities of

the affiliates may be masked at the discretion of the affiliates by the third party RPM service provider, such identities remaining anonymous if an affiliate so chooses.

Another alternative embodiment of the present invention is shown in FIG. 15. In this embodiment, any individual organization of the general public 860 may use a third party RPM service provider for provisioning resources, as opposed to vendors providing resources that are provisioned for affiliate use in a resource exchange. Here, the third party RPM service provider provides the infrastructure to allow any individual organization of the general public requiring provisioning services to obtain such services, thus providing a public provisioning infrastructure. This configuration supports customers without resources to utilize the resources of a resource exchange or other external resources that are part of a public provisioning infrastructure.

To effect the embodiment of the invention shown in FIG. 15, the third party RPM service provider may provide any individual organization of the general public 860, which includes, without limitation, users, organizations and affiliates, with a "ticket" subsequent to the verification of the user's identity. The "ticket" may associate the user with entitlement, policies, attributes, roles and rules in connection with the provisioned resources. An organization may have, for example, an "organizational footprint" that defines which of the positions in an organization are entitled to various resources and also defines the level of access to and utilization of those resources to which the particular position is entitled. For example, if a person in an organization is a salesperson, the ticket may give the salesperson access to every resource to which the salesperson is entitled based on the rules defined in the organizational footprint. So, for example, if someone obtains a ticket, that person gets footprint access into the resources of the infrastructure, or the resource exchange, made available to it by virtue of the footprint, ticket and the authenticity of the user's identification.

Tickets may be authenticated and verified by a trusted third party RPM service provider. Attributes for tickets may vary widely. A ticket may be transferable, it may exist for a specific length of time, or it may have various access rights associated with it. A ticket may exist for one person, several persons, or an entire organization. For example, suppose a law firm has a need to use a resource such as an information database. Assume that the law firm enters into an agreement with the information database resource provider and also enters

into an agreement with a trusted third party RPM service provider to provision its employees with access to the database. Then, the trusted third party RPM service provider will generate a ticket for such access. Each lawyer in the firm would then get a ticket for access to the database in accordance with firm policy. Alternatively, the entire firm may receive one ticket  
5 for access to the database. The ticket may be good for a set period of time and may provide each attorney with certain access rights with respect to the database. At the end of the set period of time, the law firm may analyze usage and cost associated with the database and modify the access rights on the ticket.

Continuing with this example, assume a new attorney joins the law firm.

10 Because the law firm has already entered into an agreement with the third party service provider to provision its attorneys with the database, and because the law firm has already entered into an agreement with the database resource provider to utilize the database, all the law firm need do to provision the new attorney with database access is to provide information to the third party RPM service provider indicating that a new attorney has joined the firm and  
15 provide the third party RPM service provider with relevant information regarding the new attorney. Because resource providers are provided with tickets, the third party RPM service provider will then generate a ticket and send it to the database resource provider. In turn, the database resource provider will set up an account for the new attorney. The new attorney may then access the database, subject only to authentication of her identity by PKI or another  
20 identity authentication method.

A flowchart detailing a method for implementing the embodiment of FIG. 15 is shown in FIG. 16. A request for provisioning services may be received by a third party RPM service provider at step 870. Such a request may be made by an individual organization in the general public needing such services. The request may be made via electronic means or by  
25 personal contact between the appropriate persons at the organization and at the third party RPM service provider. At step 872, the third party RPM service provider allocates appropriate space on its server to accommodate the data processing needs of the organization making the service request.

At step 874, the third party RPM service provider receives user information  
30 from the organization making the request. This information may include, but is not limited to,

user name, user number, a list of resources for which the user desires access, the nature of the access rights, and the like. This information may be sent electronically from the organization to the third party RPM service provider using a network, such as, for example, the Internet. The third party RPM service provider will then provision the user with the requested resources  
5 at step 876. Once the user has been provisioned with the resources, the user is at liberty to use such resources pursuant to agreements entered into between the third party RPM service provider and the individual organization and the resource provider and the individual organization.

The embodiment of FIG. 15 may be likened to a hub and spoke configuration,  
10 wherein the third party RPM service provider is the hub and groupings of affiliations or individual organizations in the general public exist at the end of each spoke. In this embodiment, all levels of access may be permitted within the confines of the public provisioning infrastructure. For example, assume that a non-computing resource such as a charge card account exists within a resource exchange of affiliated companies. If an individual  
15 organization in the general public who is not a member of the resource exchange desires to be provisioned with such charge accounts, it may enter the infrastructure by requesting that a trusted third party RPM service provider generate a ticket for it that provides it with access to the charge accounts in the exchange.

A graphical diagram showing various levels of embodiments of the present  
20 invention is shown in FIG. 17. At the central location provisioning level 880, various organizations 881 may obtain resource provisioning from a third party RPM resource provider. At an affiliate level 882, various resource vendors 883 may be part of a resource exchange, sharing resources with other affiliates 883 within the exchange. At a public provisioning infrastructure level 884, an individual organization 885 may obtain access to  
25 resources within the infrastructure, subject to receipt of a provisioning ticket and appropriate identity authentication.

The embodiments shown in FIGS. 9-17 may be used in connection with a public key infrastructure (PKI), i.e., an infrastructure providing identification authentication and certificates. Using PKI, the identity, privacy and nonrepudiation of users of embodiments of  
30 the present invention, which includes, without limitation, companies, organizations, vendors,

and affiliates, as well as members of the general public, may be assured. Once an identity is assured by PKI, provisioning of a resource for a user may occur. A provisioning infrastructure may be coupled with a PKI such that identity is authenticated and resources are provided based on the identity and the relationship between the identity and the provisioning policy of an organization making a resource available to a user. PKIs are well known in the art and will not be described in detail here. Although PKI may be part of the infrastructure utilized by a third party RPM service provider when providing its provisioning services, it may also exist as a provisionable resource within a resource exchange or a public provisioning infrastructure.

While the invention has been described with reference to its preferred embodiments, those skilled in the art will understand and appreciate from the foregoing that variations in equipment, operating conditions and configuration may be made and still fall within the spirit and scope of the present invention which is to be limited only by the claims appended hereto.

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
21